**PURPOSE**

This transmits Chapter 2, Facility and Property Protection, of new Handbook, 1.16.8, Physical Security Standards, which replaces IRM 1(16)41, Physical and Document Security Handbook.

**BACKGROUND**

The IRM is being converted to a new format and style which will be issued in 8½" x 11" instead of the current 6" x 9" size. The new IRM Handbook includes simplified text, a new numbering system, and a new format for organizing text.

The transmittal reissues existing information in the IRM format and provides new guidelines on facility, property and information protection. It replaces text currently contained in IRM 1(16)41 which is obsolete.

**NATURE OF MATERIALS**

New IRM Handbook 1.16.8, Physical Security Handbook, provides guidance and procedures for the protection of information, property and facilities.

Leland N. Keller
National Director, Real Estate
Planning and Management Division

# Table of Contents

2.1 (02/26/99)
**General**

(1) Security protection should be provided through design, technology and procedural controls which will incorporate physical, data, and space management requirements during the development, and planning phases of a facility. There are many security safeguards from which a viable security program may be developed to protect the property and personnel within a site or facility.

(2) Due to physical, operational, and financial limitations, absolute security is neither possible nor practicable. Therefore, the approach to physical security offered herein is a practical program to protect information, facilities, property and personnel by employing a combination of measures to deny, deter, detect and/or apprehend unauthorized entrants and to preserve the environment in which the Service's mission may be carried out without disruption.

(3) In addition to providing safeguards to control unauthorized access, a well balanced security program must provide measures to protect Service facilities and personnel from threats that may cause property damage or risk to life. Such measures are included in 1.16.6, Occupant Emergency Planning Handbook; 2.10.0, Automated Information Systems Security; local building, fire and electrical codes; and, this Handbook.

(4) The options available to deny, deter, detect, and/or apprehend unauthorized entrants and the required Minimum Protection Standards for certain types of Service facilities and operations are contained in Chapter 5 of this Handbook.

---

2.2 (02/26/99)
**Physical Security Planning Guidelines**

(1) Whether the activity services the public directly, or is strictly supportive in nature, the type and value of equipment, complexity of operations, concentration of tax data and the consequence of any interruptions are all vital considerations.

---

2.3 (02/26/99)
**External Environment**

(1) Major consideration in physical security planning is the general character of the external environment or neighborhood, the quantity and quality of police and fire protection afforded the immediate area should be determined. Factors such as response time, frequency of patrol and jurisdictional limitations will influence these determinations.

---

2.4 (02/26/99)
**Building Structure and Location**

(1) One of the first considerations in establishing a security program for a particular activity is the building in which the activity is located. The number of floors, doors, windows, fire exits, roof vents, the degree of ground level access and adjacent parking facilities, all affect entry control considerations. At service centers, loading docks, kitchen entrances and

boiler room doors are normally weak links in the building perimeter security. Therefore, they should be given special attention. The material structure of the building (interior partitioning, ceilings, and doors) affects the degree of security afforded contents against destruction, theft and unauthorized disclosure. If the building is not entirely occupied by the Service, the nature of operations conducted by other tenants will affect security in Service occupied space. The Consolidated Physical Security Standards for IRS Facilities should be used in determining physical security requirements.

2.5 (02/26/99)
**Interior Space Planning—Open Office Concept**

(1) The open office concept requires different security considerations from the traditional style individual office concept. In open office planning, an entire open area must be treated in its entirety with perimeter security provided that is commensurate with the security needs of the most critical operation. During operating hours, entrance areas should be arranged to control visitor access such as channeling visitors to a receptionist.

(2) Because of the increasing costs of office space, construction/alteration and the implementation of the “open office” concept, it is imperative that security considerations be addressed whenever IRS space is designed, acquired, altered or redesigned. A failure to consider adequate security during the early phases of space planning could result in the need for costly modifications after the completion of the project. In “open office” environments, we must ensure that acoustical planning guidelines are considered in order to minimize the potential for inadvertent unauthorized disclosures and to reduce ambient noise to an acceptable level. Security personnel and operational managers must be aware of the acoustical design goals for “open office” planning, and the speech privacy considerations.

(3) All managers will ensure that open office concept plans provide for:

a. Perimeter security commensurate with the needs of the most critical operation to be performed in the office;
b. Use of dividers, as appropriate, to separate operational areas and to minimize extraneous traffic;
c. Functional aural and visual privacy to minimize inadvertent disclosures of tax and privacy data; and
d. Appropriate storage for protectable items during non-duty hours.

2.6 (02/26/99)
**Alternative Duty Stations — Flexiplace**

(1) Flexiplace provides employees the opportunity to perform their duties at alternative duty stations remote to the conventional office site (e.g., satellite locations, employee’s residence). The policy of the Internal Revenue Service is to provide the highest level of protection to sensitive data, including taxpayer related information, and to assure that proper controls are in place to secure information that is being processed at

satellite locations or in the homes of employees. The standards provided in this Handbook will be applied to satellite locations and the home environment. Files containing sensitive IRS information or data will be secured when not in use or not in the possession of the Flexiplace employee. Employees are responsible for protecting all government records and data against unauthorized disclosure, access, mutilation, obliteration or destruction.

2.7 (02/26/99)
## Sensitive Areas

(1) Certain areas in the Service require more protection or are considered more sensitive due to one or more of the reasons listed below and should be given special attention during planning. The protection given sensitive areas during construction and redesign will minimize the need for costly safeguards to protect information once the areas become functional.

a. They contain large amounts of cash or negotiable instruments;
b. They contain large amounts of valuable property which can be easily stolen or damaged;
c. They contain large quantities of information requiring protection;
d. They contain protectable information in highly concentrated and easily alterable or destroyable forms;
e. Process or function being performed in the area is sensitive and must be protected;
f. Personnel in the area, due to the positions they hold (e.g., district directors and above), the functions they perform (e.g. examination, collection, investigations, etc.) or simply their physical characteristics (e.g. handicaps) may be subject to potential threats such as assault, hostage taking, robbery, etc.

(2) The following sensitive areas require minimum protective measures as listed below:

a. Computer Rooms — Computer rooms shall be slab-to-slab and where feasible should be located in a central building location away from the building exterior, parking garages or top floor locations. Computer rooms will be windowless, lockable with access control system that provides an audit trail of who was last in the area. Computer rooms are secured, restricted areas and must meet secured area standards as required in Chapter 5 of this Handbook. Access shall be controlled as required in Chapter 4 of this Handbook. (Also see National Fire Protection Association (NFPA) Standard No. 75 and IRM 2700 and 2.10.0)
b. Tape Libraries — Tape libraries shall be slab-to-slab and where feasible should be located in a central building location away from the building exterior. Tape libraries are secured, restricted areas and must meet secured area standards as required in Chapter 5 of this Handbook. Access shall be controlled as required in Chapter 4 of this Handbook. (Also see National Fire Protection Association (NFPA) Standard No. 75, IRM 2700 and 2.10.0.)
c. Telecommunications Closet — The telecommunications closet shall be slab-to-slab and shall be lockable with access permitted only authorized personnel.

d. Mechanical/Electrical Rooms — Security control and power distribution boxes and panels shall be located in secured electrical closets. Doors must be key locked, keys controlled and access limited to authorized personnel only.
e. Child Care Facility — If child care facilities are located at IRS facility, they shall be protected with a duress alarm capability serving only that space. Entry to the child care center shall be through a reception room. Entry from the reception area to the rest of the child care center shall be controlled by an electric lock operated from the reception area. Penetrations from the child care center into the IRS facility shall be minimized and shall be alarmed and on an access control system.

(3) Exhibit 1.16.8.2–1 is a listing of some of the areas which should be given extra security. Traditionally, many or all of these areas have been protected during working hours by making them restricted areas. This Handbook recognizes that the restricted area concept for protection during working hours and the secured area concept for protection during non-working hours are but two ways of achieving required security.

---

2.8 (02/26/99)

## National Office Headquarters — Protective Measures

(1) Protective measures in the National Office are the responsibility of the Director, Support and Services Division. All managers are responsible for the proper protection of documents and information within their areas of responsibility. This handbook and the Consolidated Physical Security Standards for IRS facilities provide guidance in selecting appropriate security measures.

(2) At a minimum, the following measures will be employed in the National Office:

a. Guard service for the main building and, where feasible, satellite buildings will be provided;
b. During non-duty hours, the building will be locked and entry controlled. Individuals desiring entrance will be required to enter the designated entrance, show identification to the security guard, and sign the register;
c. All entrances will be locked or protected by a security guard during duty hours and all employees will be required to show identification at the designated entrance(s) to gain entry to the building;
d. ID cards will be worn by all employees while in Service controlled space;
e. Inspection of packages and briefcases of visitors and vendors entering and exiting the building will be conducted;
f. Where feasible, random inspection of packages and briefcases of employees entering and exiting the building will be conducted;
g. During heightened security, inspection of packages and briefcases of all employees entering the building will be conducted;

h. Secured areas, following the same procedures provided in Chapter 4 of this document, may be established to assist division directors in providing better security to those areas requiring more than normal protection;
i. Restricted areas will use restricted area designators assigned to district offices and the same procedures provided in Chapter 4 of this document will be followed for restricted areas;
j. An Occupant Emergency Plan (see 1.16.6) will be maintained to provide instructions to be followed during an emergency. The Commissioner, as the designated official in charge of National Office Buildings, during an emergency situation has designated the Director, Support and Services Division as the coordinator to develop and maintain the overall plan of action.

---

2.9 (02/26/99)
**Regional Office Protective Measures**

(1) The Regional Director, Support Services, or the designated host site chief, is responsible for the protective measures at the regional facility.

(2) A regional office will normally not contain large amounts of tax information; however, careful planning is necessary to ensure that the office, as a vital link in the Federal Tax Administration System, is properly protected. Because of the wide variance of facilities, the protection of regional offices cannot be standardized. Planning for the offices located in a Federal buildings may be somewhat easier than for offices located in leased space, which may require a different approach. The protective measures for the National Office (section 2.8 of this Chapter) may be used as a guide where appropriate. In addition, the Consolidated Physical Security Standards for IRS Facilities provide guidance on selecting appropriate security measures.

(3) Restricted areas will use restricted area designators assigned to district offices and the same procedures provided in Chapters 4 and 5 of this document will be followed for restricted or secured areas.

---

2.10 (02/26/99)
**Service Center Protective Measures**

(1) As one of the most vital activities within the Service, particular attention must be given to developing a well-rounded, sound physical security program for each service center. In addition to this handbook, guidance can be found in the Consolidated Physical Security Standards for IRS Facilities, IRM 2700 (Information Systems Operations and Management Handbook), 2.10.0 (Automated Information Systems Security Manual) and the National Fire Protection Association (NFPA) Standard No. 75.

(2) To provide a minimum acceptable level of protection the following measures will be implemented at each service center:

a. Uniformed guard;
b. Two-way radio communication capability for guards;
c. Exterior protective lighting;

d. Security glass in all main building entrance doors, sidelights, transoms, and guard houses;
e. Visitor control;
f. Electronic intrusion detection system;
g. Proprietary protection console for on-site systems monitoring and response;
h. Contingency plans to cope with emergencies;
i. Local emergency exit alarms;
j. Duress alarms (or other means of communication) from console to police department, fixed posts at building entrances and fence gates to console, and computer area to console (if desired by local IRS management);
k. Sprinkler protection for returns files and warehouse areas;
l. Sprinkler water flow alarms and supply valve supervision;
m. Manual fire alarm and evacuation system;
n. Exterior fire service loop and hydrants;
o. Industrial protection and supervision of boiler, electrical distribution, computer room temperature and humidity, and power to computer room;
p. Emergency “path-of-light” lighting and exit lights above each fire exit.

(3) The provisions of the National Fire Protection Association (NFPA) Standard No. 75, Standard for the Protection of Electronic Computer/Data Processing Equipment, and RP–1, Standard Practice for the Fire Protection of Essential Electronic Equipment Operations will be followed as minimum guides. The following additional protective systems will be installed in all computer room/library areas and site adapted to suit local conditions without sacrificing basic protective measures:

a. Separately valved wet pipe, water sprinkler system (pipe scheduled or hydraulically designed type) inside the entire firewall, encapsulated computer room and tape library areas with automatic power cut-off capability (National Fire Protection Association (NFPA) Standard No. 13 provides details on installation of acceptable sprinkler systems);
b. Manual fire alarm and evacuation system with pull boxes at each door leading out of the encapsulated area;
c. A system to continuously monitor all electronic detection, extinguishing, and environmental and utility support systems to detect abnormal conditions;
d. One hour fire resistive separation of the computer (electronic equipment) area perimeter from adjoining areas to protect the electronic equipment from the damaging effects of a fire which may occur outside the equipment area;
e. Air conditioning and ventilating systems shall be in compliance with Section 301 of RP–1 and NFPA Standard No. 90A to ensure that the systems are designed to prevent the spread of fire, smoke and fumes from exposed areas into the computer room or tape library;
f. A computer complex water flow device, which will automatically disconnect the power to all electronic equipment in the computer area and to the air conditioning system serving the area. When the sprinkler test drain is turned on, the water flow device must

disconnect the power to all equipment and air conditioning within 30 seconds. This is necessary to remove the heat/ignition source, to minimize the transfer of smoke to other areas and to limit the spread of combustion by avoiding “fanning” the fire with fresh air. If local water supply pressure surges present a problem in meeting this requirement of 30 seconds, the National Office should be consulted for remedial advice. All power must remain off until manually reset.

g. Emergency shut-down push buttons (controls) must be installed at each principal computer complex exit. When activated, they must disconnect the power to all electronic equipment in the computer area and to the air conditioning system serving the area (section 303 of RP–1 and text 8–4.1 NFPA No. 75);
h. Floor drains or sump pumps to provide water drainage in the event of a sprinkler head activation or a plumbing leak above the ceiling or under the floor (section 202–4, 203.3.c and 205–4 of RP–1, and section 2.2 of Federal Information Processing Standards (FIPS) Pub. 31 (Guidelines for Automatic Data Processing Physical Security and Risk Management);
i. Sprinkler shut-off valve (also called OS&Y) that controls the sprinkler system to the computer and/or library (section 702 of RP–1 and section 2.1.3 FIPS Pub 31). For additional information on actions to be taken by computer personnel in emergencies, see section 705 and Chapter VIII of RP–1 and Section 2.1.4 and Chapter 8 of FIPS Pub 31;
j. Plastic waterproof covers stored at some convenient location for use in case of an emergency (FIPS Pub 31 and section 202.4, 803–3 and 803–5 of RP–1);
k. Ionization systems in each computer room/tape library and ionization detector heads must be installed above suspended ceilings (unless ceiling is fire rated), on suspended ceilings and below elevated floors. Each ionization system must be properly engineered (must have a maximum of 400 square feet coverage per ceiling mounted detector) and there should be separate zones (change-of-state alarm modules) on the on-site protection console to indicate alarm conditions and supervisory service (trouble conditions) for each ionization system. (If ionization systems do not meet the above criteria, authority should be obtain from GSA for local IRS management to install or upgrade the systems.)
l. Floor lifting devices mounted immediately adjacent to each portable fire extinguisher must always be readily available;
m. Class A and Class C fire extinguishers prominently located within the computer complex so that an extinguisher is available within 50 feet of travel (section 704 of RP–1 and section 2.1.3 of FIPS Pub 31);
n. Emergency “Path-of-Light” lighting and exit lights above each fire exit;
o. Room temperature and humidity supervision devices that will detect an abnormal temperature or an abnormal humidity condition within the area. Each device must be separately annunciated on the on-site protection console;

p. Sensors to detect power failure of main feeder supplying computer power systems with appropriate annunciation on the on-site protection console;
q. An audible sounding device (alarm) for each room within the firewall encapsulated area of the computer complex that will alert the complex that unauthorized person(s) have entered the area. Alarms will be activated from the protection console (if desired by local IRS management);
r. Main doors to computer areas and libraries, which may be automatic, electric, or pneumatically powered horizontal bi-parting sliding doors, provided the integrity of the firewall is maintained;
s. At least one standard single or double set of out swinging doors in computer area;
t. Computer room doors secured against unauthorized or casual passage.

(4) Due to the nature of the ionization smoke detection system installed in computer rooms and tape libraries, it is necessary to prohibit smoking in these areas. The use of any type of smoking material such as cigarettes, cigars and pipes within the firewall encapsulated area is not authorized. **It is up to the manager of the computer room to ensure compliance with this procedure.**

(5) All computer room and tape library personnel should be periodically instructed on the location of power down buttons, sprinkler shut off valves, waterproof covers (see 1.16.6), floor pullers and fire extinguishers and, as deemed appropriate by local management, should be given experience in the use of such protective devices. They should also be informed of when and how such devices should be used.

(6) In order to ensure the proper function or availability of systems and devices, it is necessary that they be inspected and/or tested on a periodic basis. This is the responsibility of the manager of the computer room. The items below will be inspected or tested as follows:

a. All systems in (1)(f), (g), (l), (j), (k), (l), (m), (n), (o) and (p) above must be tested at least annually to ensure that they function properly.
b. All systems in 2(a), (b), (c), (f), (h), (k), (n) and (q) above must also be tested at least annually to ensure that they function properly.
c. The floor drains, (2)(h) above, must be checked at least annually to ensure that they have not become clogged. If sump pumps have been installed, they will be tested at least annually to insure that they are functional.
d. The floor lifting devices, (2)(l) above, must be checked at least semiannually to ensure that they are still present.
e. All fire extinguishers, (2)(m) above, must be inspected at least annually.

(7) Only approved self-extinguishing type trash receptacles shall be used in computer rooms.

2.10.1 (02/26/99)
**Perimeter Security**

(1) Each service center will be protected by a perimeter security fence with appropriate gates to allow pedestrian and vehicular traffic to enter the facility on a controlled access basis.

(2) Initial control for entry into a service center will be exercised at the fence line. Each fence opening will be protected by a guard when not closed and locked. All persons entering the property on foot must be identified through the display of an IRS photo identification card or as an authorized visitor. Persons in vehicles will be permitted to enter if they display (where feasible) the authorized IRS photo identification card and if the vehicle has an authorized vehicle identification sticker (see section 2.10.7). Visitors will be directed to the entrance designated for visitors, where they will be issued a visitor identification card.

(3) Primary entry control will be maintained at the building perimeter. All doors will be protected by a guard when not closed, locked and protected by an intrusion alarm system. All employees entering the building will be identified by an IRS photo identification card which must be worn in accordance with requirements in 1.16.4. At a minimum random screening of employees will be conducted. Authorized visitors will enter a designated entrance and, upon verification of identity (photo ID), be issued a visitor identification card prior to entering the remainder of the building. All visitors will be screened and packages/briefcases will be examined. The issuance of identification cards will be in accordance with 1.16.4.

(4) Loading docks, kitchen entrances and boiler room doors are normally weak links in building perimeter security. The installation of fencing around these entrances with the gates alarmed and with gates controlled by guards strengthens the security in these areas. During daylight hours, the building perimeter at these entrances is extended to these inner fence lines. After dark, the applicable building entrances are closed, locked and alarmed.

2.10.2 (02/26/99)
**Security Guard Service**

(1) The only effective means to control access to large facilities is through the use of a uniformed guard force. The guard force is supplemented by a variety of security systems. Security systems may reduce the number of guard personnel necessary; however, guards cannot be eliminated entirely because a response capability is necessary to answer alarm situations.

(2) An annual 24-hour post consists of 8,760 staff hours. Since a guard works 1,770 productive staff hours yearly, it takes five guards to cover one annual 24-hour post. As a minimum, security guards will be assigned to the following 24 hour posts at each center:

- a perimeter fence gate;
- 24 hour building entrance;
- proprietary protection console;
- internal patrol; and
- external patrol

(3) In addition to the minimum coverage, additional security guards will monitor each open (unlocked) gate and each open (unlocked) exterior door of the building. All gates and doors must be protected by a security guard whenever they are not locked and/or protected by an electronic intrusion detection system.

(4) Armed guards they will be properly trained and certified in the use of firearms. Each security guard may carry a holstered firearm at all times while on duty. The firearm is to be drawn as a last resort—only in a defensive situation for the protection and defense of life. The firearm is never to be left unattended, even momentarily.

(5) A full-time, on-site contract supervisor will be on duty at each center. Duty hours will normally coincide with the main shift operation at the service center. In addition, each guard shift will have a responsible supervisor on-site. The position of a security guard and a supervisor cannot be held by the same individual. This does not preclude a supervisor from assisting security guards in the performance of their duties during temporary emergencies.

(6) The Security staff will coordinate with GSA to establish monitoring procedures and ensure that GSA takes appropriate follow-up action against the contractor.

2.10.2.1 (02/26/99)
**Contract Security Officer Inspection**

(1) An agreement between GSA and IRS regarding the administration of contracts for guard service at the IRS service centers gives the Service the responsibility for contract inspection (CI) within the administration of security protective service contracts. The agreement provides that the Service can review a contractor's performance, talk directly to the contractor's on-site representative, and recommend deductions from payments to the contractor for non-performance.

(2) The agreement also gives the Service the right to conduct the government portion of the officers training. The Service has the right to utilize the tenured officer proficiency examination to determine which officers need training and which officers may have training waived.

(3) Under the agreement, the Service (National Office) has the right to provide input to GSA in the development of the Public Buildings Service guide specifications/solicitations for armed guard service. The field security functions will not request the GSA regions to delete or add to the guide specifications without IRS National Office approval.

(4) It is the responsibility of the Host Site Chief to ensure that the center(s) for which they are responsible has all the provisions of the guide specifications in the center contract; act as liaison between the GSA regional office and the center; provide the Real Estate Planning and Management Division a copy of the current guard contract for each service center and computing center for which they are responsible; and ensure compliance with the requirements of and provisions contained in this Chapter.

2.10.2.1.1 (02/26/99)
**Contract Inspection**

(1) Contract Inspectors (CI's) will be appointed by the host site chief. Most appointees should be from the security function. Should additional CI's be needed to cover weekends, holidays, or non-prime time shifts, other functions in the center that have employees present during those times can submit a list of their employees to the director for consideration and appointment.

(2) Once all CI's have been designated, the list will be sent to the GSA Contracting Officer (CO) in the GSA Regional Office servicing that center. The CO will formally appoint the CI's by a letter to each CI and a copy to the Contracting Officer's Representative (COR) and the Contractor (see Exhibit 1.16.8.2–2).

(3) Training the CI's is the responsibility of the CO; however, the CO usually delegates this to the COR, who is generally a Federal Protective Officer (FPO). GSA has developed a training course for this purpose. Though it is usually administered by GSA personnel, under the following circumstances, IRS Security personnel who have been given GSA approved CI training, may conduct CI training of other Service personnel. After the initial training of all CI's, replacement CI's may be trained by the Security function, provided approval is obtained from the CO. GSA has the right to monitor any or all of the CI training and has agreed to provide assistance when requested by the IRS.

(4) The host site chief will appoint a primary CI. The primary CI will be responsible for, but not limited to, the following activities:

a. Make out the schedule of inspections to be done by the CI's.
b. Provide a copy of the schedule of inspections to the COR at least one week in advance of the inspections.
c. Receive and review the inspection report from all CI's.
d. Follow up on discrepancies reported on inspection reports with the contractor's on-site representative to ensure that discrepancies have been corrected.
e. File a copy of the inspection report and forward the original inspection report to the COR.
f. Attend post-award conference.
g. Administer the tenured officer proficiency examination to all officers who qualify and have successfully completed the weapons firing.
h. Receive all forms (e.g. firearms qualification, pistol permit, medical examination, etc.) from the contractor and forward to the COR.
i. Keep records of all forms submitted by the contractor for each officer.
j. Act as liaison between the COR and all other CI's.
k. Request all GSA forms needed from the COR.
l. Make recommendations for deductions to the COR from CI inspection reports.
m. Schedule all government provided officer training and monitoring contractor provided training.
n. Keep training records on each officer — number of hours each officer is in training, test scores of each officer and subjects waived on each officers.
o. Control the training tests.

p. Notify the COR of completed training requirements for each officer.
q. Verify officer training hours against invoice from the contractor.
r. Ensure all CI's have been trained and appointed by the CO.
s. Keep in each officer's file the notification from GSA that the officer has a completed, satisfactory background check.
t. Inventory all weapons authorized on-site at least once a month.
u. Inspect or observe the inspection of firearms in storage at least twice a month for cleanliness and proper operation.
v. Ensure that contract security personnel are using the clearing barrel to load/unload weapons.
w. Ensure that contract security personnel do not remove weapons from the IRS premises.

(5) Individual CI's will conduct inspections as directed by the primary CI, using the locally developed inspection form or the inspection form provided by GSA in accordance with the service center procedures.

(6) All CI's will complete an inspection form immediately after or during the inspection of the security force shift. The CI's will deliver a copy of the inspection report to the contractor's on-site supervisor and ask him/her to correct any deficiencies noted. Should the deficiency be serious enough (e.g. post abandoned, officer sleeping, etc.) the CI will immediately notify the contractor's on-site supervisor for corrective action. If immediate action is not taken by the contractor's on-site supervisor, the CI will notify the primary CI or the COR depending on local procedures. The original inspection report will be delivered to the primary CI in the Security function.

(7) CI's should never touch an officer or his/her equipment; direct the officer to do a specific task (except in an emergency); inspect his/her weapon or ammunition while it is in his/her possession; or refer to a deduction from the contract payment as a penalty. Violations of any of these could result in a legal action by the officer and/or contractor against the CI, the IRS and/or the United States Government or be in derogation of rights or remedies otherwise available to the government.

(8) Any proposal for a reduction or increase of contract security hours/costs should be reported by the security function to the GSA regional contracting officer so he/she can plan for the necessary contract changes.

(9) For the first thirty (30) days of a new contract, the officers should be inspected every shift, every day. (This will consist of at least ninety (90) inspections.) After the first 30 days of the new contract, the inspections can be dropped to a minimum of sixty percent or twelve (12) inspections per week. These 12 inspections must be conducted on varying days, on varying shifts, and at varying times of the shifts to be effective. This does not mean that every officer on duty must be completely inspected each shift. Should any problems with security officers occur, the inspections can be accelerated at local option.

(10) CI's will not inspect a weapon which has been issued to an officer and is in the possession of the officer. Non-security CI's will not inspect weapons or ammunition. Because circumstances, conditions and situations vary at the IRS centers, the following are options authorized by the IRS National Office and GSA Central Office for weapons and ammunition inspection:

a. The CI (security function only) may inspect the weapons and ammunition in storage for cleanliness and proper operation at least twice a month; or
b. The local Federal Protective Officer (FPO), if he/she desires, may inspect the weapons and ammunition in storage for the IRS; however, if this procedure is used the IRS primary CI must accompany the FPO at least twice a month and observe the FPO inspecting the weapons and ammunition for cleanliness and proper operation; or
c. The contractor's on-site supervisor may inspect the weapons and ammunition in storage for the IRS; however, if this procedure is used, the primary CI must accompany the contractor's on-site supervisor at least twice a month and observe the supervisor inspecting the weapons and ammunition for cleanliness and proper operation.

2.10.3 (02/26/99)
**Interior Security and Control**

(1) Each Service Center Director will institute such internal controls beyond the minimum as are necessary to properly protect the Tax Administration System and preserve the confidentiality of the tax return and related documents.

(2) Control of the internal movement of personnel within a center is necessary to ensure that only authorized Service personnel are permitted in critical areas and that visitors do not wander throughout the service center. The personnel identification card has been designed to assist management in maintaining this internal control.

(3) Each service center will administer the personnel identification card program, which will permit entry only to authorized personnel. The system as specified in 1.16.4 is also designed to assist management in controlling movement within the service center. All employees are required to wear the authorized Service ID cards while in the center.

(4) The need to maintain reasonable security at service centers at all times requires that only authorized visitors be permitted to enter the center. Providing tours for interested non-tax related individuals or groups for purposes of orienting them with service center operations is not authorized. Official visits by individual tax preparers, tax accountants, news media representatives and other professional tax oriented individuals and groups may be permitted at the discretion of the director and in keeping with security interests.

2.10.4 (02/26/99)
**Restricted Area**

(1) The designation of restricted area is a method of controlling the movement of individuals and eliminating unnecessary traffic through

critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of tax information. The basic requirements are contained in Chapter 4 of this Handbook.

(2) A distinctive colored identification card as specified in 1.16.4 will be worn at all times by all personnel within each restricted area.

2.10.5 (02/26/99)
**Secured Area**

(1) The following are designated as secured areas, in addition to being restricted areas, and admittance is permitted only on a need to enter basis for all personnel not regularly assigned to work in the area:

- computer room
- tape library
- mail extraction operation
- clearing and deposition function
- remittance processing area
- returns files
- microfilm section of Research Branch

(2) Incoming mail not being distributed or processed will be stored in a secured area or in locked containers when possible. Mail, incoming and outgoing, will not be left unattended in areas open to the public.

(3) The requirements and standards for secured areas are contained in Chapter 5 of this Handbook.

2.10.6 (02/26/99)
**Remittance Processing Areas**

(1) The entire area will conform to restricted area criteria as outlined in Chapter 4 of this Handbook. Keys and lock combinations to cash drawers, cash boxes and the security containers will be strictly issued and controlled as outlined in Chapter 4 of this Handbook.

(2) The remittance clerk will lock the cash drawers and remove the key when leaving the area. The remittance clerk will empty cash drawers and will store cash boxes in an appropriate container at the end of each workday (see Exhibit 1.16.8.5–2).

2.10.7 (02/26/99)
**Vehicle Identification**

(1) If a perimeter fence is used at a service center, proper vehicle identification is required for entering the property. This can be accomplished by guards checking ID cards (where feasible) and/or vehicle identification stickers (decals) of adequate size and reflectivity. Stickers must have a serial number and should not display anything that would identify it with the Internal Revenue Service or the center. Vehicle identification stickers, when used, will meet the following specifications:

a. Materials used in stickers will be reflective vinyl;
b. Dimensions — 2 3/4″ X 4 3/4″
c. All printing (including serial numbers) 1 1/2″ high;
d. Style of printing — block letters in upper case;
e. Colors may be used to further identify owners of registered vehicles;

f. Stickers should be designed so that they cannot be reused when removed.

(2) Stickers will be placed so that they can be readily seen by the guard. At the discretion of the Director and depending on state and local laws stickers may be placed on either rear side windows, front or rear windows, or any other prominent location.

(3) The Office of Security is responsible for development, implementation, maintenance and control of the vehicle identification system. At locations where employees pay for parking, a windshield permit can be used (see paragraph 10 below).

(4) Records of all stickers issued and their disposition (i.e. lost, stolen, destroyed) will be maintained by the Security office.

(5) The vehicle identification sticker records will consist of a record by serial number of completed “Vehicle identification Sticker Request” cards. Records will at a minimum show sticker serial number, name of the employee to whom the sticker was issued, the employee branch or section, year and make of the car, the date of issue, date of disposition and type of disposition. Destruction of unusable vehicle identification stickers (i.e. mutilated, misprinted, etc) should also be recorded.

(6) Concurrent with the issuance of an identification sticker, the employee will be informed of the requirement to remove and return the sticker or remains to the issuing office prior to selling or trading the vehicle, or if that area on the vehicle where the sticker is affixed is damaged and replaced. In addition, the security office must be informed when the sticker is destroyed, lost or stolen.

(7) The sticker will be removed from vehicles of employees who terminate employment at the center. The sticker will then be destroyed.

(8) Stickers will be replaced at least every two (2) years. Color scheme and designation should be varied each time the stickers are changed.

(9) At the discretion of the center Director, vehicle passes, logs, written advance notice of visits, etc. can be used to pass vehicles of employees who have not been issued a sticker, visitors and vendors through gates. Below is a recommended system of doing this:

a. Temporary vehicle passes may be issued to employees who do not have vehicle ID stickers, providing they show an authorized Service ID card. A log will be maintained by the security guard showing vehicle pass number, name of employee, vehicle license number and date of issue. The temporary pass must display the license plate number, expiration date, and permit number. If an employee does not have a proper Service ID card, their employment status will be verified by checking with the appropriate IRS supervisor. Temporary vehicle passes for employees may not exceed 30 days. If necessary, the permit may be reissued after the 30 day period.

b. Visitors can be issued a Visitor Vehicle Pass. Visitors must show a picture ID and must be on an access list. The vehicle pass may not be used for in and out access, but rather the visitor must show a picture ID and be checked against the access list each time he/she enters. A Visitor Vehicle Pass is good for one day only and must be dated. The vehicle pass will be recovered by the guard at the end of the day.
c. Temporary Vehicle Passes may be issued to vendors and others requiring access. These individuals must show a picture ID and must be on an access list. The vehicle pass may not be used for in and out access and is good for one day only and must be dated. The vehicle pass will be recovered by the guard when individuals exit facility.

(10) If identification of employee vehicles is going to be made by use of the parking permit (that is cannot be adhered to the vehicle to prevent tampering) in lieu of vehicle identification stickers or windshield decals, these permits will be issued monthly, will be of a different color each month, will be serial numbered and employee will show Service identification card to gain access. The Security office will follow the procedures stated above on issuance, records maintenance and recovery.

---

2.11 (02/26/99)
## Martinsburg Computing Center (MCC) Protective Measures

(1) The activities performed at MCC are unique and vital to the mission of the Service. The nature and significance of MCC operations require the implementation and maintenance of a sound physical security program.

(2) To provide a minimum acceptable level of protection the protective measures outlined in section 2.10 will be implemented and maintained at the Martinsburg Computing Center.

2.11.1 (02/26/99)
### Perimeter Security

(1) MCC is protected by full-time, uniformed, armed IRS police officers as authorized by GSA.

(2) The MCC will be protected by a perimeter security fence with appropriate gates to allow pedestrian and vehicular traffic to enter the facility on a controlled access basis. At all times when fence gates are open, uniformed, armed security guards will monitor each opening to ensure against unauthorized entry.

(3) Initial control for entry into the Martinsburg Computing Center will be exercised at the fence line. Each unlocked gate will be protected by a uniformed officer. All persons entering the property on foot must display a Service photo identification card or be identified as an authorized visitor. Persons in vehicles will be permitted to enter if they display an authorized Service photo identification card or if the uniformed officer has their name on a preclearance listing. Vehicle identification stickers, decals, or cards are not required. Visitors must show photo identification (such as a driver's license) to verify identity.

(4) Loading docks, kitchen entrances, and boiler room doors are normally weak links in building perimeter security. The installation of fencing around these entrances with the gates alarmed and with the gates controlled by uniformed officers strengthens the security in these areas. During daylight hours the building perimeter at these entrances is extended to the inner fence line. After dark, the applicable building entrances are closed, locked and alarmed.

2.11.2 (02/26/99)
**Interior Security and Control**

(1) Control of the internal movement of personnel is necessary to ensure that only authorized Service personnel are permitted in critical areas and that visitors do not wander throughout the building. The personnel identification card has been designed to assist management in maintaining this internal control.

(2) The MCC will administer the personnel identification card program which will permit entry only to authorized personnel. The system as specified in 1.16.4 is also designed to assist management in controlling movement within the center.

(3) Requests for tours of the facility should be made in writing and sent to the Chief of the Security function. The tour participants must be listed in the request and identities confirmed (thru use of photo ID's) at the onset of the tour. Tours of the facility (except the computer area) require the approval of the Director of MCC.

(4) Tours of the computer area require approval of the Chief, Systems Operations Branch, and the Director of MCC. A senior official must conduct the tour.

2.11.3 (02/26/99)
**Restricted Areas**

(1) The designation of restricted areas is a method of controlling the movement of individuals and eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of tax information. The basic requirements are contained in Chapter 4 of this Handbook.

(2) A distinctive colored identification card as specified in 1.16.4 will be worn at all times by all personnel within each restricted area.

2.11.4 (02/26/99)
**Secured Area**

(1) The following are designated as secured areas, in addition to being restricted areas. Personnel not regularly assigned to work in these areas will be admitted only on a need-to-know basis.

- computer room
- computer library

2.12 (02/26/99)
**Detroit Computing Center Protective Measures**

(1) The activities performed at the Detroit Computing Center (DCC) are unique to the Service. The nature, volume and significance of the work performed there requires a complete, practical, and sound physical security program.

(2) To provide a minimum acceptable level of protection, the protective measures outlined in section 2.10.2 of this Chapter will be implemented and maintained at the Data Center.

2.12.1 (02/26/99)
**Perimeter Security**

(1) The parking area of the DCC will be protected by a perimeter security fence with gates which allow traffic to enter the facility on a controlled access basis. Uniformed and armed security guards will monitor each gate at all times when they are open. Vendor and visitor parking spaces will be designated and in view of a security guard.

(2) In addition to the parking lot security guard, there will be a uniformed and armed security guard at each unlocked/unalarmed entrance to the building to control access.

(3) Persons in vehicles will be permitted to enter if the vehicle has an authorized vehicle sticker, windshield decal, or card. Where feasible, in addition to the authorized vehicle sticker, employees will display the authorized Service ID card. Persons in vehicles without authorized stickers (vendors, visitors, etc.) will be permitted to enter after the security guard confirms authority of person(s) to enter the facility and after the individual shows a picture ID (e.g. drivers license) verifying identity.

(4) All pedestrians entering the facility will be identified by displaying an IRS photo identification card or confirmed as an authorized visitor and displaying a photo ID verifying identity. Employees requiring temporary replacement identification cards and authorized visitors will be directed to the reception desk in the building lobby for entry registration and issuance of an appropriate identification card.

2.12.2 (02/26/99)
**Interior Security and Control**

(1) The Detroit Computing Center Director will institute any necessary controls beyond the minimum that are necessary to properly protect the operations of the center and the confidentiality of the records being processed.

(2) Control of the internal movement of personnel is necessary to ensure that only authorized personnel are permitted in critical areas and that visitors do not wander throughout the building. The personnel identification card has been designed to assist management in maintaining this internal control.

(3) Tours of the facility (except the computer area) are allowed if the request is received in writing by the Chief of the Security function, the participants' identities are confirmed, and the request is approved by the Director.

(4) Tours of the computer area are allowed under the following conditions:

a. The Director, Assistant Director, or designee is conducting the tour; or
b. Prior approval is received through the Chief, Systems Operations Branch, from the Director or designee, and a senior official conducts the tour.

2.12.3 (02/26/99)
**Restricted Area**

(1) The designation of restricted areas is a method of controlling the movement of individuals and eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of tax information. The basic requirements are contained in Chapter 4 of this Handbook.

(2) A distinctive colored identification card as specified in 1.16.4 will be worn at all times by all personnel within each restricted area.

2.12.4 (02/26/99)
**Secured Areas**

(1) The following are designated as secured areas in addition to being restricted areas. Personnel not regularly assigned to work in the area will be admitted only on a need-to-enter basis.

- Computer Room
- Computer Library
- Four Phase key-to-disc Conversion Area
- Error Resolution Section Document Storage Room
- Mail/Receipt Room

(2) The requirements and standards for secured areas are contained in Chapter 5 of this Handbook.

---

2.13 (02/26/99)
**District Office Protective Measures**

(1) To ensure that the district office (protective measures applied to district offices will also apply to all other sites, i.e. client sites, annexes, etc. not described in this chapter) is properly protected careful planning is necessary to ensure that appropriate protective measures are in place. These offices will vary greatly in size and function and so each will require close individual examination. The function of the office, the type of documents and records maintained, and equipment will be determining factors in how much security is required. The need for security guard service, electronic protective systems, restricted areas and secured areas will have to be evaluated on an individual basis. In determining protective measures, Chapters 4 and 5 of this Handbook and the Consolidated Physical Security Standards for IRS Facilities should be considered.

2.13.1 (02/26/99)
**Teller Operations**

(1) Certain minimum physical security measures are required to protect currency and other negotiable items received by the teller. These measures include the following:

a. The teller operation may be located in the same area as other taxpayer assistance operations, however, direct access to the teller area will be physically limited by bank-type counters, counter-high partitions, lockable half doors, or some similar type of construction that provides equal protection. When this operation is located on the ground floor of a building with windows to the exterior grade level, windows will be alarmed.
b. The exact construction of the teller area and the type of security container needed will depend on the average daily receipts, the location of the IRS office, and other appropriate security considerations. For this reason, Facilities Management Branch will be consulted before making any changes to the teller area.
c. The use of appropriate duress alarm systems should be considered for these areas. The alarm will annunciate at the control center (FPO, local police, etc.) or may alarm in the Inspection or Criminal Investigation function if such office is located on-site and has a response team available.
d. Money chests, vaults or cabinets affording adequate security (see Chapter 5 for requirements) must be available for deposit activities in a designated area of the district office.
e. Each teller will be provided with a separate money bag, cash box, or compartment (depending on the protective facilities used) which opens with a separate key or combination. Each teller may also be furnished the combination to the safe.

(2) Excess currency will not be kept in the teller area. As often as business permits, currency in excess of the change making fund will be transferred to a security container. It is preferable to have this located in a room away from the teller area. However, if this cannot be accomplished, the Security staff will be consulted for assistance in determining the most secure alternate location.

a. Whenever a teller operation area is left unattended, tellers' cash drawers or boxes must be locked in the safe and all protectable items must be containerized. During a teller's brief absence, when the area is unattended, that teller's cash drawer or box must be locked and the key removed.
b. Cash drawers will be emptied, and cash boxes stored in the security container at the end of each workday.
c. After the balancing operation has been completed, the cash must be kept in a locked container to await deposit. The key to that container should be held by the teller's immediate supervisor.

(3) Keys and lock combinations for cash drawers, cash boxes and the security containers will be protected, controlled, and changed as outlined in Chapter 4 of this handbook.

a. If it becomes necessary to open a teller's locked compartment in the absence of the teller, the manager will select two responsible employees to use the duplicate key or combination. They must count the money and documents found, sign the statement and attach it to the receipt that the teller previously signed for the change fund.

b. The duplicate keys to tellers' cash containers and the copy of the combination to the safe or vault are not to be in the possession of the same employee.

(4) Managers will make quarterly unannounced reviews of the physical and fiscal security of teller operations. Each review will be documented by a memorandum report to the local Security office.

(5) "Received" and "received with remittance" stamps will be assigned to specific individuals and a record kept by serial number of each assignment. Form 1930, Custody Receipt for Government Property, will be used for recording these assignments. The number of stamps in each office will be held to a practical minimum. Each individual to whom a stamp is assigned should furnish sufficient physical protection to safeguard against unauthorized or indiscriminate use. When a stamp is not in use, it will be stored in a locked container under the exclusive control of the individual to whom the stamp is assigned. Where this is not practical, special care must be exercised to ensure against unauthorized use. The face of each stamp will be inscribed with the following elements:

- Internal Revenue Service;
- Received;
- Month, Day, Year;
- District Director (city, state); and
- Stamp Serial Number

2.13.2 (02/26/99)
**Restricted and Secured Areas**

(1) Consolidated files areas (formerly Centralized Services Branch) will be maintained as a restricted and secured area until all files and functions have been dispersed. Admittance will be permitted only on a "need to enter" basis for all personnel not regularly assigned to the work area. (See Chapters 4 and 5 for the criteria for a restricted area and a secure area.)

2.13.3 (02/26/99)
**Protection of Mail**

(1) Incoming mail, not being distributed or processed, will be stored in a secured area or in locked containers when possible. Mail, incoming and outgoing, will not be left unattended in areas open to the public

2.13.4 (02/26/99)
**Computer Rooms**

(1) The provisions of National Fire Protection Association (NFPA) Standard No. 75, Protection of Electronic Data Processing Facilities and RP–1, Standard Practice for Fire Protection of Essential Electronic Equipment Operations, will be followed as minimum guidelines for all computer rooms. Computer rooms will be slab-to-slab and where possible should be located in a central building location away from the building exterior, parking garages or top floor locations; they should be windowless, lockable and alarmed. Computer rooms are secured, restricted areas and should follow standards as stated in Chapters 4 and 5 of this Handbook).

2.14 (02/26/99)
**Off-Site Facilities**

(1) Protection provided off-site facilities will depend on the use that is made of the space. The need for security guard service, electronic protective systems, restricted areas and secured areas will be evaluated on an individual basis.

**Exhibit 1.16.8.2-1 (02/26/99)**
**Areas Requiring Special Security Considerations**

1. COMPS Room
2. Candling Area
3. Computer Room
4. Computer Tape Library
5. Criminal Investigation Work Area*
6. Mail Extraction Work Area
7. Mailroom
8. Microfilm Area
9. Proprietary Console Room
10. Remittance Processing Work Area
11. Returns Files
12. Teller Area
13. ACS Call Sites

*If the CID area is designed to meet all the requirements of a restricted area, and if within that CID area a restricted area is established for Grand Jury material, only one of those restricted areas will require the use of a Restricted Area Register at its entrances. However, wherever the Grand Jury area is located, it is very important that during working hours, the material shall not be left unattended. After work hours, the material shall be properly stored in a security container or in a security room.

**Exhibit 1.16.8.2-2 (02/26/99)**
**Agreement Between IRS and GSA**

AGREEMENT BETWEEN THE INTERNAL REVENUE SERVICE (IRS)
AND THE GENERAL SERVICES ADMINISTRATION (GSA)
REGARDING THE ADMINISTRATION OF CONTRACTS FOR
GUARD SERVICE AT THE IRS SERVICE CENTERS

**INTRODUCTION**

This agreement sets forth the responsibilities and obligations of each agency in the procurement and administration of contracts for armed guard service at the IRS Service Centers.

**AUTHORITY**

This agreement is entered into pursuant to the Federal Property and Administrative Services Act of 1949 as amended.

**BACKGROUND**

Recognizing the need to prevent disruption to the Nation's revenue collection system and the responsibilities of the IRS to keep the system functioning on a continuing tight schedule, the GSA and the IRS agree on the need for providing effective protection for the key IRS data processing facilities. The IRS understands the broad responsibilities of GSA regarding the protection of Federal property and personnel. At the same time, the GSA recognizes the vital concern of the IRS over the quality and duties of the contract security guards assigned to these facilities. The IRS is specifically charged to protect tax data, etc., in the Internal Revenue Code.

Therefore, in the best interest of the Government, both agencies mutually agree to the principles outlined herein regarding the protection of the facilities.

**SCOPE OF PROJECT**

This agreement covers the contracts for guard service at the following IRS Service Centers and includes all service center off-site facilities now in existence, or that may be added in the future.

1. Internal Revenue Service Center
   310 Lowell Street
   Andover, MA 01810
2. Internal Revenue Service Center
   1040 Waverly Avenue
   Holtsville, NY 11742
3. Internal Revenue Service Center
   11601 Roosevelt Blvd.
   Philadelphia, PA 19154
4. Internal Revenue Service Center
   201 W. Rivercenter Blvd.
   Covington, KY 41019
5. Internal Revenue Service Center
   4800 Buford Highway
   Chamblee, GA 30341
6. Internal Revenue Service Center
   5333 Getwell Road
   Memphis, TN 38118
7. Internal Revenue Service
   Detroit Computing Center
   985 Michigan Avenue
   Detroit, MI 48226
8. Internal Revenue Service Center
   2306 E. Bannister Road
   Kansas City, MO 64131
9. Internal Revenue Service Center
   3651 Interregional Highway
   Austin, TX 78742
10. Internal Revenue Service Center
    1160 West 1200 S. Street
    Ogden, UT 8201
11. Internal Revenue Service Center
    5045 E. Butler Avenue
    Fresno, CA 93888

**RESPONSIBILITIES**

The GSA will:

1. Maintain the overall responsibility for the physical protection of the facilities.

2. Investigate crimes reported by IRS.

3. Issue traffic and parking tickets through the use of mobile patrols when required to do so by IRS.

4. Respond to emergency situations resulting from a contractors failure or inability to perform.

5. Maintain the normal mobile response capability at the facilities.

6. Require its personnel (FPO's, building personnel and maintenance personnel, etc.) To comply with IRS entry control procedures.

**Exhibit 1.16.8.2-2 (Cont. 1) (02/26/99)**
**Agreement Between IRS and GSA**

7. Be totally responsible for procuring armed guard service at the locations specified above. GSA will make the final determination as to the type of contract, method of procurement, etc. it is understood that GSA will comply with all applicable Federal Acquisition Regulations.

8. Consider the views and desires of the IRS (National Office) in the development of PBS guide specifications/solicitations for armed guard service. Suggestions by IRS for revisions to the guide specification will be considered when they are submitted.

9. Consult with designated regional IRS representatives on the requirements of the individual contracts during solicitation.

10. Retain the overall responsibility for administration of the contracts awarded for the IRS service centers. This is an inherent responsibility of the contracting officer. The regional contracting officer will designate a Federal protective Service employee, named by the Regional director, FPDS, as the “contracting officer representative.”

The contracting officer will also designate IRS employee(s) named by the IRS Service Center designated officials, as contract inspectors. The duties and responsibilities of the contracting officer, contracting officer’s representative, and contract inspectors are outlined on Attachment 1 to this Agreement. The contracting officer will make these designations, in writing, and will fully inform the designees of their duties, responsibilities, and limitations. The letters of designation shall read substantially the same as the samples included as Attachments 2 and 3 to this Agreement.

11. Revoke the designation of any COR or CI who fails to properly carry out his/her responsibilities.

12. Provide the IRS with copies of the contracts, handbooks, GSA forms, etc., necessary for the IRS representatives to carry out its responsibilities.

13. Promote a cooperative relationship with the IRS personnel in an effort to strive to achieve quality guard service at the centers for the overall interests of the U.S. Government.

14. Train IRS employees designated to serve as contract inspectors on GSA’s contract inspection procedures. The GSA contracting officer may authorize IRS to train the inspectors, provided GSA is informed of the training schedule so that the training may be monitored by GSA.

15. Allow IRS to conduct the government provided training to the contract security guards. GSA reserves the right to monitor all training, Government and contractor provided. The IRS will solicit GSA’s cooperation and assistance in providing training on subjects such as Orders for Posts, report writing, security and other building systems.

The IRS will:

1. Reimburse GSA for the cost of service provided in excess of that which is provided by GSA under the Federal Buildings fund. The amount of reimbursement will be based on the GSA contract costs.

2. Cooperate with the GSA in the development and revision of the PBS guide specifications/solicitations for guard services to ensure a uniform nationwide approach to guard service requirements.

3. Cooperate with the regional GSA contracting officer in developing the requirements for individual contract requirements.

4. Designate IRS representatives to serve as contractor inspectors. The responsibilities of the contract inspectors are outlined in Attachment 1.

5. Promote a cooperative relationship with GSA personnel in an effort to strive to achieve quality guard service at the centers for the overall interest of the U.S. Government.

6. Provide training materials for use in training contract guards.

7. Submit all records accumulated in connection with the inspection or the contract to the GSA COR for forwarding to the contracting officer for retention with the official contract documents.

8. Solicit GSA's cooperation and assistance in conducting the Government provided training to contract security guards.

9. Comply with Federal Property management Regulations (FPMR) requirements for reporting crimes to the Federal Protective Service.

**Exhibit 1.16.8.2-2 (Cont. 2) (02/26/99)**
**Agreement Between IRS and GSA**

10. All GSA personnel into IRS spaces based on a need to enter following the visitor guidelines in Chapter 2 of this handbook.

**TERMINATION**

This agreement may be terminated by either GSA or IRS upon 90 days notice.

Attachment 1

Duties and Responsibilities of Officials Involved in Contract Inspection and Administration

**1. General** — The term "contract administration" covers a broad range of activities that take place between contract award and contract completion. The purpose of contract administration is to see that the Government receives the services for which it has contracted, on time, and in accordance with specifications. In order to have an effective contract administration program, all Government employees involved in contract administration must work as a team. Therefore, it is imperative that Government employee who is involved in the process know and understand his/her role and responsibilities.

**2. Contracting Officers** — The contracting officer has the overall responsibility for administration of the contracts he/she awards. However, because a contracting officer is responsible for all other aspects of the acquisition process and is involved in or responsible for a number of contracts which may involve work at a number of different geographic locations, he/she must rely on the individuals who he/she authorizes to act as his/her representative. A contracting officer may delegate certain responsibilities to his/her authorized representatives (COR's and CI's). Those responsibilities which are normally delegated are outlined in paragraph 3 and 4 below. The contracting officer must retain or reserve certain authorities and responsibilities for himself/herself. The contracting officer must:

a. Authorize start of work;

b. Interpret the terms and conditions of the contract when disputes arise between Government inspectors and the contractor;

c. Authorize any deviation from the contract terms and conditions.

d. Make final decisions with respect to disputed deductions from contract payments for the contractor's failure or omission;

e. Determine suitability of contract employees;

f. Inform the contractor of his/her obligation to comply with the applicable labor laws;

g. Withhold monies from payments for labor violations;

h. Authorize the assignment of payments to a third part;

i. Amend or modify the contract requirements;

j. Issue cure notices;

k. Terminate the contract for default or the governments convenience;

l. Assess excess additional procurement costs;

m. Negotiate termination settlements;

n. Issue final decisions regarding contract questions or matters under dispute; and

o. Resolve any disputes between the contracting officer's representative and the contract inspectors.

**3. Contract Officer's Representative (COR)** — When the contracting officer is unable to be directly in touch with the contract work, he/she must designate, in writing, a representative to assist him/her in the discharge of responsibilities. The responsibilities include, but are not limited to, the following:

a. Being thoroughly familiar with the contract requirements and specifications;

b. Scheduling and attending pre-work conferences;

c. Interpreting drawings and specifications;

d. Advising the contracting officer when the contractor fails to begin work in accordance with the schedule provided in the contract;

e. Personally inspect the work on a periodic basis as well as ensure that the work is being inspected by the IRS contract inspectors. The COR will coordinate on-site visits, inspections, etc., with the contract inspectors and advise the IRS contract inspectors of the results of all inspections;

**Exhibit 1.16.8.2-2 (Cont. 3) (02/26/99)**
**Agreement Between IRS and GSA**

f. Promptly advising the contracting officer if the contractor fails to remove, correct, or replace rejected guards, uniforms, equipment, or service;

g. Advising the contracting officer of any factors which may cause delay in performance of work;

h. Supplying the contract inspectors with necessary handbooks, forms, etc.;

i. Collecting the security clearance forms from the contract inspectors and forwarding the forms to the central office Federal Protective Service for processing. The COR will notify the IRS contract inspector of the results of suitability clearance, i.e., suitable or unsuitable;

j. Maintaining official files of the Firearms Qualifications Forms, health certificates, training certificates, etc. These forms will be collected by the contract inspectors and submitted to the COR for retention during the contract period. Upon expiration of the contract, all records will be turned over to the contracting officer;

k. Notifying the contractor in writing of proposed deductions from contract payments for the contractors failures or omissions and of the right to appear. Copies of proposed deduction letters shall be provided to the contracting officer and the IRS contract inspector. All appeals regarding proposed deductions shall be decided by the contracting officer. This responsibility may not be redelegated by the contracting officer; and

l. Recommending termination of contracts for default.

**4. Contract inspectors (CI)** — Contract inspectors are responsible for the day-to-day inspection and monitoring of the contractor's work. The responsibilities of the contract inspectors include, but are not limited to, the following:

a. Being thoroughly familiar with the contract requirements and specifications;

b. Inspecting the work, uniforms, and equipment at least once per relief, per day to ensure compliance with the contract requirements;

c. Documenting through written inspection reports the results of all inspections conducted. Copies of inspection reports shall be provided to the contractor's on-site representative as well as the COR;

d. Promptly report to the contracting officer's representative any problems with regard to the quality of work, timely delivery of services, etc;

e. Following through to ensure that all defects or omissions noted on inspection reports are corrected or completed;

f. Conferring with representatives of the contractor regarding any problems encountered in the performance of the work. All discussions shall be with the contractor's on-site representative or officers of the company. The contract inspectors shall not directly or indirectly supervise the contractor's employees:

g. Collecting security clearance forms, health certificates, firearms qualifications forms, etc., from the contractor and forwarding them to the COR for processing.

h. Recommending to the COR appropriate deductions from contract payments for the contractor's failure or omissions; and

i. Generally assisting the COR in carrying out his/her responsibilities.

IRS contract inspectors **will not**, under any circumstance, inspect a weapon which has been issued to a guard and is in the possession of the guard. The IRS non-security contract inspectors **will not** inspect weapons or ammunition at any time.

Because circumstances, conditions, and situations vary at the IRS service centers, the following options are offered for inspecting weapons:

a. The IRS contract inspector (security function only) inspects the weapons and ammunition in storage for cleanliness and proper operation at least twice a month.

**Exhibit 1.16.8.2-2 (Cont. 4) (02/26/99)**
**Agreement Between IRS and GSA**

b. The COR or his/her representative may, if he/she desires, inspect the weapons and ammunition in storage for the IRS at least twice a month. However, the IRS primary contract inspector must accompany the COR or his/her representative during the inspection.

c. The IRS contract inspector may observe the contractor's on-site supervisor inspect the weapons and ammunition in storage at least twice a month.

d. If weapons cannot be inspected while in storage, they shall be inspected in an area away from the public and building occupants. Weapons shall not be inspected while guards are on post.

**Exhibit 1.16.8.2-2 (Cont. 5) (02/26/99)**
**Agreement Between IRS and GSA**

Attachment 2

| | | |
|---|---|---|
| General | Public | |
| Services | Buildings | |
| Administration | Service | Washington, DC 20405 |

**SAMPLE LETTER**

Date:

Reply to Attn of: Contracting Officer

Subject: Contract No. _____, Guard Service, location_____

To: (Name of Contracting Officer Representative)

The purpose of this memorandum is to formalize the appointment as Contracting Officer Representative for the subject contract.

1. Broadly, the Contracting Officer Representative's prime responsibilities are to ensure that the contractor's efforts comply with the technical features of the work required by the referenced contract and include the following:

a. Being thoroughly familiar with the contract requirements and specifications.

b. Scheduling and attending pre-work conference.

c. Interpreting drawings and specifications.

d. Advising the Contracting Officer when the contractor fails to begin work in accordance with the schedule provided in the contract.

e. Personally inspect the work on a periodic basis as well as ensure that the work is being inspected by the IRS Contract Inspectors. The COR will coordinate on-site visits, inspections, etc., with the Contract Inspectors and advise the IRS Contract Inspectors of the results of all inspections.

f. Promptly advising the Contracting Officer if the contractor fails to remove, correct, or replace rejected work.

g. Advising the Contracting Officer of any factors which may cause delay in performance of work.

h. Supplying the Contract Officer of any factors which may cause delay in performance of work.

**Exhibit 1.16.8.2-2 (Cont. 6) (02/26/99)**
**Agreement Between IRS and GSA**

Attachment 2–cont.

i. Collecting the security clearance forms from the Contract Inspectors and forwarding the forms to the Central Office Federal Protective Service for processing. The COR will notify the IRS Contract Inspector of the results of suitability clearance, i.e. suitable of unsuitable.

j. Maintaining officials files of the Firearms Qualifications Forms, health certificates, training certificates, etc. These forms will be collected by the contract inspectors and submitted to the COR for retention during the contract period. Upon expiration of the contract, all records will be turned over to the Contracting Officer.

k. Notifying the contractor, in writing, of proposed deductions from contract payments for the contractor's failures or omissions and of the right to appeal. Copies of proposed deduction letters shall be provided to the Contracting Officer and the IRS Contract Inspector. All appeals regarding proposed deductions shall be decided by the Contracting Officer. This responsibility may not be redelegated by the Contracting Officer.

2. Recommending termination of contracts for default — In no event shall appointment as Contracting Officer Representative empower the recipient to:

a. Issue contract changes, deviate from the terms and conditions of the contract, or take action on matters involving contract modifications, extension of time, claims, or disputes.

b. Manage the contractor's efforts.

c. Supervise or otherwise control the contractor's employees.

d. Perform any other function which would validate the provisions of the contract.

This appointment shall become effective not he effective date of the contract and shall not be redelgated. It shall remain in effect until rescinded in writing.

Contracting Officer

cc: Contractor

**Exhibit 1.16.8.2-2 (Cont. 7) (02/26/99)**
**Agreement Between IRS and GSA**

Attachment 3

| | | |
|---|---|---|
| General | Public | |
| Services | Buildings | |
| Administration | Service | Washington, DC 20405 |

**SAMPLE LETTER**

Date:

Reply to Attn of: Contracting Officer

Subject: Contract No. _____, Guard Service, location _____

To: (Name of Contract Inspector(s))

The purpose of this memorandum is to formalize your appointment as Contract Inspector for the Subject contract.

Contract inspectors are responsible for the day-to-day inspection and monitoring of the contractor's work. The Contract inspector's duties and responsibilities include the following:

a. Being thoroughly familiar with the contract requirements and specifications.

b. Inspecting the work, uniforms and equipment at least once per shift, per day for the first 30 days of a new contract to ensure compliance with the contract requirements. After the first 30 days of a new contract, assuming the contractor's performance is satisfactory, the inspections may be reduced to a minimum of 60 percent or 12 inspections per week. These inspection shall be conducted on varying days, on varying shifts, and at varying times during the shift. The primary contract inspector for the IRS shall periodically provide the COR with a schedule of which shifts will be inspected by the IRS inspectors. The schedule shall be provided one week prior to the period covered by the schedule. This will enable GSA personnel to inspect guards on shifts the IRS will not be monitoring.

c. Documenting through written inspection reports, the results of all inspections conducted. Copies of inspection reports shall be provided to the contractor's on-site representative as well as the COR.

d. Promptly reporting to the Contracting Officer's Representative any problems with regard to the quality of work, timely delivery of services, etc.

e. Following through to assure that all defects or omissions noted on inspection reports are corrected or completed.

f. Conferring with representatives of the contractor regarding any problems encountered in the performance of the work. All discussions shall be with the contractor's on-site representative or officers of the company. The contract inspectors shall not directly or indirectly supervise the contractor's employees.

**Exhibit 1.16.8.2-2 (Cont. 8) (02/26/99)**
**Agreement Between IRS and GSA**

Attachment 3–cont.

g. Collecting security clearance forms, health certificates, firearms qualifications forms, etc, from the contractor and forwarding them to the COR for processing;

h. Recommending to the COR appropriate deductions from contract payments for the contractor's failure or omissions.

i. Generally assisting the COR in carrying out his/her responsibilities.

In no event shall appointment as Contract Inspector empower the recipient to:

a. Issue contract changes, deviate from the terms and conditions of the contract, or take action on matters involving contract modifications, extension of time, claims, or disputes.

b. Manage the contractor's effort.

c. Supervise or otherwise control the contractor's employees.

d. Perform any other function which would violate the provisions of the contract. This appointment shall become effective on the effective date of the contract and shall not be redelegated. It shall remain in effect until rescinded in writing.

Contracting Officer

cc: Contractor
Contracting Officer's Representative